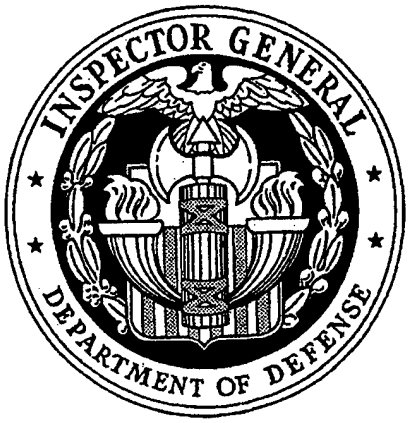
Audit Report



U.S. EUROPEAN COMMAND YEAR 2000
OPERATIONAL READINESS

Report No. 00-004 October 8, 1999

Office of the Inspector General
Department of Defense

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932 or visit the Inspector General, DoD, Home Page at www.dodig.osd.mil.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

CTAPS	Contingency Theater Automated Planning System
JOA	Joint Operations Area
MESL	Master Events Sequence List
NATO	North Atlantic Treaty Organization
NEO	Non-Combatant Evacuation Operation
USAREUR	U.S. Army, Europe, and Seventh Army
USEUCOM	U.S. European Command
Y2K	Year 2000

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-2884

October 8, 1999

MEMORANDUM FOR COMMANDER IN CHIEF, U.S. EUROPEAN COMMAND

SUBJECT: Audit Report on U.S. European Command Year 2000 Operational Readiness (Report No. 00-004)

We are providing this report for information and use. We considered U.S. European Command comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the audit staff. Questions on the audit should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) (eklemstine@dodig.osd.mil) or Ms. Catherine M. Schneiter at (703) 604-9614 (DSN 664-9614) (cschneiter@dodig.osd.mil). See Appendix D for the report distribution. The audit team members are listed inside the back cover.

Robert J. Lieberman

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. 00-004
(Project No. 8LG-5039.02)

October 8, 1999

U.S. European Command Year 2000 Operational Readiness

Executive Summary

Introduction. This is one in a series of reports being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the year 2000 computing challenge. For a listing of audit projects addressing the issue, see the year 2000 web pages on the IGnet at http://www.ignet.gov/.

The U.S. European Command conducted its operational evaluation in three parts. Part I, conducted in May 1999, assessed the ability of the U.S. European Command to support land and sea operations. Part II, conducted jointly with the Air Combat Command assessment of the Air Operations Center in June 1999, assessed the ability of the U.S. European Command to support air operations. Part III, conducted in August 1999, assessed the ability of the U.S. European Command to support intelligence activities.

Objectives. The overall audit objective was to evaluate whether year 2000 risks had been adequately planned for and managed to avoid undue disruption to the U.S. European Command's mission. The specific audit objective was to evaluate the effectiveness of the U.S. European Command year 2000 operational evaluation to test its thin-lines of systems critical to performing non-combatant evacuation and peacekeeping operations.

Results. When initially audited, the U.S. European Command had completed its operational evaluation of land, sea, and air operations. Since the time of the draft report, the U.S. European Command completed its operational evaluation of intelligence operations. The U.S. European Command operational evaluation verified that its mission-critical systems used to support non-combatant evacuation and peacekeeping operations were functionally ready to operate in a year 2000 environment. In addition, the U.S. European Command, in coordination with the Joint Staff, the Services, and the Principal Staff Assistants, reviewed the results of the Service-sponsored systems integration tests and the functional area end-to-end tests and verified that the systems tested were also functionally ready to operate in a year 2000 environment. The combined results from the operational evaluation, the Service-sponsored systems integration tests, and the functional area end-to-end tests provided the U.S. European Command with sufficient information to determine that it should be operationally ready to perform non-combatant evacuation and peacekeeping operations in the year 2000 and beyond. However, the U.S. European Command needs to continue to take action through its risk mitigation efforts to reduce any potential impact on its ability to conduct peacekeeping operations caused by year 2000 interoperability problems with North Atlantic Treaty Organization and coalition forces.

The U.S. European Command planned to complete its risk mitigation efforts in October 1999 to ensure that potential year 2000 failures will result in as little disruption as possible. See the Finding section for details.

Summary of Recommendation. We recommend that the U.S. European Command's risk mitigation efforts include a focus on the year 2000 compliance of North Atlantic Treaty Organization and coalition forces' mission-critical systems supporting peacekeeping operations in the European theater.

Management Comments. The U.S. European Command generally agreed with the report. The U.S. European Command stated that it had successfully completed Part III of the operational evaluation on intelligence systems at the Joint Analysis Center, August 13 through August 16, 1999. Therefore, we deleted a draft recommendation that Part III be completed. In addition, the U.S. European Command stated that its risk mitigation efforts encompass contingency planning for infrastructure and host nation support risks to operations and to life support of military communities, assurance of continuity of operations of ongoing operations, and engagement with the North Atlantic Treaty Organization and coalition forces' risk mitigation activities. The U.S. European Command stated that a number of information sources were being tapped, including U.S. intelligence sources, to assess the risks. However, in recognition of the limited information available on the actual status of other nations' command and control systems, planning by the U.S. European Command and its Service Components will continue to include the risk that all or parts of those systems may not be available. In its determination of the risks to be mitigated, the U.S. European Command will include all available data on the compliance of North Atlantic Treaty Organization and coalition forces' mission-critical systems with which the U.S. European Command must interoperate. The U.S. European Command Year 2000 Task Force and Supreme Headquarters Allied Powers Europe Year 2000 Programme Management Office are exchanging information on the status of systems as data become available. A discussion of management comments is in the Finding section of the report and the complete text is in the Management Comments section.

Table of Contents

Background

Office of the Secretary of Defense Memorandum. The Deputy Secretary of Defense issued a memorandum, "Year 2000 (Y2K) Verification of National Security Capabilities," August 24, 1998, directing the Principal Staff Assistants of the Office of the Secretary of Defense to verify that all functions under their purview will continue unaffected by year 2000 (Y2K) issues. The Services and Defense agencies were required to test the information technology and national security system Y2K capabilities of their respective Component systems in accordance with DoD guidance. In addition, each Principal Staff Assistant was required to provide the Deputy Secretary of Defense with plans for Y2K-related end-to-end testing of each process to address communications, health and medical, intelligence, logistics, and personnel operations. Further, the test plans were to include all mission-critical systems involved in each test. The Directorate of Operational Test and Evaluation, Office of the Secretary of Defense, was to help the Principal Staff Assistants with cross-functional, inter-Service, and cross-system testing.

DoD Y2K Management Plan. In his role as the DoD Chief Information Officer, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) is coordinating the overall DoD Y2K conversion effort. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) issued the "DoD Year 2000 Management Plan, Version 2.0" (DoD Management Plan), December 1998, revised June 8, 1999, to provide direction and make DoD Components responsible for implementing the five-phase Y2K management process. The goal of the DoD Y2K program is to ensure the continuance of a mission-capable force able to execute the National Military Strategy before, on, and after January 1, 2000, unaffected by the failure of mission-critical or support systems to properly process date-related information. The DoD Management Plan directs the unified commands to conduct operational evaluations to identify specific Y2K problems, to establish workarounds where feasible, and to suggest contingency approaches for ensuring that essential operations will continue without interruption. It also requires that the Services conduct Service-sponsored systems integration tests and that the Principal Staff Assistants conduct functional area end-to-end tests.

Joint Staff Operational Evaluation Guidance. The "Joint Staff Year 2000 Operational Evaluation Guide, Version 3.0" (Joint Staff Guide), April 1, 1999, provides guidance to assist the unified commands in tailoring exercises, demonstrations, or experiments to conduct Y2K operational evaluations for mission-critical systems. Operational evaluations are designed to assess the ability of certified Y2K compliant systems to support joint and combined operations from sensor-to-shooter under conditions replicating a Y2K environment. The Joint Staff is responsible for providing guidance to the unified commands on planning, executing, evaluating, and reporting on operational evaluations.

U.S. European Command. The U.S. European Command (USEUCOM) is one of nine unified commands of DoD. On October 1, 1998, the USEUCOM area of responsibility expanded from 83 to 89 countries with the addition of 6 former states of the Soviet Union. A primary mission of USEUCOM is to provide combat forces to the North Atlantic Treaty Organization (NATO). In addition, USEUCOM conducts operations unilaterally or in concert with coalition partners. Service Components provide forces, as required, to support USEUCOM operations. The USEUCOM Service Components are the U.S. Army, Europe, and Seventh Army (USAREUR); U.S. Naval Forces Europe; U.S. Air Forces in Europe; U.S. Marine Forces Europe; and the U.S. Special Operations Command Europe. At the September 1998 Joint Staff Operational Evaluation Conference, the Joint Staff tasked USEUCOM to perform an operational evaluation on its non-combatant evacuation operation (NEO)[1] and peacekeeping operation[2] critical missions.

Objectives

The overall audit objective was to evaluate whether Y2K risks had been adequately planned for and managed to avoid undue disruption to the USEUCOM mission. The specific audit objective was to evaluate the effectiveness of the USEUCOM Y2K operational evaluation to test its thin-lines of systems critical to performing NEO and peacekeeping operations. Inspector General, DoD, Report No. 99-145, "Year 2000 Issues Within U.S. European Command and Its Service Components," April 30, 1999, addressed the overall audit objective. See Appendix A for a discussion of the audit scope and methodology and Appendix B for a summary of prior coverage.

[1]A NEO is an operation conducted to relocate threatened non-combatants from locations in a foreign country. Those operations normally involve U.S. citizens whose lives are in danger and may also include selected foreign nationals.

[2]Peacekeeping operations are military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement.

Status of Operational Evaluation

When initially audited, USEUCOM had completed its operational evaluation of land, sea, and air operations. Since the time of the draft report, USEUCOM completed its operational evaluation of intelligence operations. The USEUCOM operational evaluation verified that its mission-critical systems used to support NEO and peacekeeping operations were functionally ready to operate in a Y2K environment. In addition, USEUCOM, in coordination with the Joint Staff, the Services, and the Principal Staff Assistants, reviewed the results of the Service-sponsored systems integration tests and the functional area end-to-end tests and verified that the systems tested were also functionally ready to operate in a Y2K environment. The combined results from the operational evaluation, the Service-sponsored systems integration tests, and the functional area end-to-end tests provided USEUCOM with sufficient information to determine that it should be operationally ready to perform NEO and peacekeeping operations in the year 2000 and beyond. However, USEUCOM needs to continue to take action through its risk mitigation efforts to reduce any potential impact on its ability to conduct peacekeeping operations caused by Y2K interoperability problems with NATO and coalition forces. USEUCOM planned to complete its risk mitigation efforts in October 1999 to ensure that potential Y2K failures will result in as little disruption as possible.

Testing Guidance

DoD Testing Guidance. The DoD Management Plan requires that all mission-critical systems that DoD expects to use in a major theater of war be tested twice in end-to-end testing and that all other mission-critical systems be tested at least once in end-to-end testing. End-to-end testing should be constructed so that it evaluates the Y2K impact on a mission or a core business process from beginning to end. The end-to-end tests should be conducted through unified command operational evaluations, Service-sponsored systems integration tests, or functional area end-to-end tests. Those three types of Y2K tests collectively are expected to cover all Y2K events necessary to demonstrate the Y2K readiness of DoD missions and functions. The DoD Management Plan allows an organization to rely on testing performed by other organizations to complete the assessment of operational capabilities.

Unified Command Operational Evaluations. Unified commands are required to conduct operational evaluations to identify specific Y2K problems, to establish workarounds where feasible, and to suggest alternative and contingency approaches to ensuring uninterrupted critical operations. The DoD Management Plan requires unified commands to test mission-critical systems supporting the most critical DoD warfighting missions and functions in operational evaluations. If those systems are not tested in a unified command operational evaluation, then they must be tested in a Service-sponsored systems integration test or a functional area end-to-end test.

Service-Sponsored Systems Integration Tests. The Services are responsible for conducting Service-sponsored systems integration tests. Specifically, the Services are responsible for the implementation, execution, testing, and operational performance of Y2K efforts within their respective Components. The Services are required to:

- execute corrective actions to ensure Component-wide Y2K compliance;
- conduct systems-level tests to validate compliance of systems that have been repaired and participate in functional and mission-level testing; and
- inform organizations that are dependent on a system about the status of Y2K efforts affecting that system so the using organization can plan accordingly.

In addition, the Services are responsible for planning, executing, evaluating, and reporting on all mission-critical systems not specifically tested in unified command operational evaluations. The Services are also responsible for testing all interfaces to each of their systems to ensure Y2K compliance.

Functional Area End-to-End Tests. The Principal Staff Assistants are responsible for verifying that all functions under their purview will continue unaffected by Y2K issues. Specifically, the Principal Staff Assistants are responsible for assessing their functional area to determine the Y2K operational readiness of their primary functions. The assessment process requires the identification of core processes, systems, and interfaces; an assessment of readiness for those systems and interfaces to support scheduled Y2K events; and the evaluation of unified command and Service testing and results.

Joint Staff Operational Evaluation Guidance. The Joint Staff Guide provides direction to unified commands on conducting operational evaluations for critical missions. It states that the objective of an operational evaluation is to verify that a unified command can successfully perform its missions, functions, and tasks in a Y2K environment. However, the Joint Staff Guide allows an organization to rely on testing performed by other organizations to complete the assessment of operational capabilities. The Joint Staff Guide identifies five phases of an operational evaluation and specifies what activities should be completed during each phase.

Identification Phase. During the identification phase, unified commands should establish a Y2K task force, identify critical missions and critical tasks, list the systems that support each critical mission and task, and determine the events to include in the operational evaluation. Inspector General, DoD, Report No. 99-145, "Year 2000 Issues Within U.S. European Command and Its Service Components," April 30, 1999, fully addressed this phase.

Planning Phase. During the planning phase, the Y2K task force should develop an operational evaluation plan. The plan should outline responsibilities for each participating Component; identify resource issues; require that

participating Components develop contingency plans, identify risks, and identify the need for simulation equipment; and include a data collection and analysis plan. In addition, the plan should identify the critical date crossings to be tested during the operational evaluation. The Joint Staff Guide required the unified commands to test date crossings from December 31, 1999, to January 1, 2000; February 28, 2000, to February 29, 2000; and February 29, 2000, to March 1, 2000. Inspector General Report No. 99-145 partially addressed this phase in a discussion of the initial USEUCOM operational evaluation plan and the status of USEUCOM contingency planning.

Execution Phase. During the execution phase, the Joint Staff Guide recommends that the unified commands execute the operational evaluation in four segments: rehearsal, baseline operations, Y2K operations, and recovery.

Rehearsal Segment. Unified commands conduct the rehearsal segment to ensure that all mission-critical systems and interfaces in the system architectures are operating correctly and to review responsibilities and checklists. During the rehearsal, unified commands exercise the data collection plan, confirm and document system configurations, and update operational and systems architectures.

Baseline Operations Segment. Unified commands conduct the baseline operations segment to capture data for comparison with data captured during the Y2K operations segment. During the baseline operations segment, operators execute the Master Events Sequence List (MESL),[3] data collectors collect and archive data, and analysts assess the databases to determine whether the data collected is accurate.

Y2K Operations Segment. Unified commands conduct the Y2K operations segment to evaluate how systems function through critical date crossings identified in the Joint Staff Guide. During this segment, operators execute the MESL, data collectors collect and archive data, and analysts assess the databases to determine whether the data collected is accurate. In addition, operators execute operational contingency plans if system failures occur, and participants meet each day to discuss the status of systems, any concerns about the MESL, and the collection of data.

Recovery Segment. Unified commands conduct the recovery segment to ensure that all data needed to perform an assessment of its Y2K operational readiness was collected. In addition, all systems must be reset to current-day operations to avoid contamination of real-world data with Y2K operational evaluation test data.

Analysis Phase. Unified commands analyze data during and after the operational evaluation. The data is analyzed to determine whether failures are Y2K related, to categorize failures as either hard or soft failures, and to determine the impact of failures on the mission.

[3]A listing that sequences the functional events of the operational evaluation. Each functional event has an operator script, which is linked through a supporting database to the MESL.

Hard Failures. Hard failures result in obvious adverse impacts on systems. Examples of hard failures include systems shutting down or displaying erroneous data.

Soft Failures. Soft failures are failures that are not obvious. An example of a soft failure would be a system that displays nine enemy tracks; when it passes the information to another system, the receiving system displays eight tracks. Analysts normally discover soft failures when they compare data from transmitting and receiving systems. Soft failures are often identified after the unified command has completed the operational evaluation.

If unified commands identify hard or soft failures during the operational evaluation, data collectors complete data collection forms, evaluate whether the failure is related to Y2K, and assess how the failure impacts critical missions.

Reporting Phase. Once the operational evaluation is complete, unified commands prepare preliminary and final reports on the results of the operational evaluation. The preliminary report, due to the Joint Staff within 7 calendar days after the operational evaluation, identifies the operational evaluation, points of contact, critical missions and tasks, thin-lines of systems, preliminary system evaluations, hard and soft failures, and recommended actions to correct problems. The Joint Staff provides a database file that the unified commands should use to prepare the preliminary report. The final report, due to the Joint Staff within 30 days after the operational evaluation, is prepared using the same format as the preliminary report. The final report, however, contains final system evaluations and unified commands are required to complete all fields in the database file.

USEUCOM Operational Evaluation

The USEUCOM operational evaluation verified that many of its mission-critical systems used to support NEO and peacekeeping operations were functionally ready to operate in a Y2K environment. USEUCOM adequately planned and executed its operational evaluation according to the Joint Staff Guide.

Planning the Operational Evaluation. USEUCOM adequately planned its operational evaluation. As part of the planning process for its operational evaluation, USEUCOM held three conferences. During those conferences, USEUCOM identified the strategic and operational tasks, mission-critical systems, and critical date crossings; selected events required to accomplish the missions; developed a methodology to ensure that dates were properly advanced; developed a data collection and analysis strategy for validating information flow; prepared an operational evaluation plan; and ensured that participants developed contingency plans.

Initial Planning Conference. In December 1998, USEUCOM held its initial planning and concept development conference for the operational evaluation. USEUCOM required that its Service Components define the scope

of Component participation, identify strategic and operational tasks to be included in the operational evaluation, and coordinate Service Component input to the operational evaluation concept of operations. At that conference, the Service Components provided a preliminary listing of their thin-lines of mission-critical systems and operational architectures.

Mid Planning Conference. In February 1999, USEUCOM held its mid planning conference. Conference participants reviewed and modified the draft USEUCOM operational evaluation plan and completed the identification of critical tasks and the associated mission-critical systems supporting those tasks. In addition, they identified the geographical locations that would participate in the operational evaluation, identified staffing requirements for those locations, and prepared a preliminary communications network plan.

Final Planning Conference. In March 1999, USEUCOM held its final planning conference. At that conference, the Service Components provided USEUCOM with their final thin-lines of mission-critical systems supporting each strategic and operational task and their contingency plans. In addition, the Service Components provided systems architectures, final communications plans, and final operational evaluation locations. During the conference, participants completed and validated the MESL. USEUCOM validated the MESL by ensuring that each event had a sender and a receiver, each data request had a corresponding data receipt, and each change to a database had a task to verify the change. USEUCOM also validated the manning requirements for the operational evaluation.

Executing the Operational Evaluation. Because of real-world operations, USEUCOM decided to conduct its operational evaluation in three parts: land and sea operations, air operations, and intelligence operations. The operational evaluation replicated the European Theater Command Center; the headquarters for the Service Components; four deployed Service Component joint task forces; and a Survey and Assessment Team.[4] NATO and coalition forces did not participate in the operational evaluation. During the operational evaluation, USEUCOM had staff in place that collected data, archived and reviewed the collected data, documented system configurations, approved changes to baseline configurations, completed MESL events, and implemented contingency plans when system failures occurred. For the land, sea, and air parts, we observed that USEUCOM and its Service Components performed date rollovers on the mission-critical systems for the three required date crossings and collected data that was used to assess that the systems were able to perform in a Y2K environment. We did not observe the intelligence part of the operational evaluation.

Land and Sea Operations-Part I. USEUCOM successfully completed Part I of its operational evaluation in May 1999. Part I primarily assessed the ability of USEUCOM to support land and sea operations and was conducted at the Warrior Preparation Center, Einsiedlerhof Air Station, Germany. USEUCOM conducted Part I using 12 response cells at 8 locations in Europe,

[4]A Survey and Assessment Team is a joint special operations task force composed of special operations units from more than one Service, formed to carry out a specific special operation.

the United States, and a ship in the Mediterranean Sea. During the rehearsal, baseline operations, and Y2K operations segments, participants completed 95 scripted events from the MESL using 20 thin-lines of systems to assess the ability of USEUCOM to perform the strategic and operational tasks related to land and sea operations for NEO and peacekeeping operations. See Appendix C for a listing of the strategic and operational tasks assessed.

Part I Rehearsal Segment. During the rehearsal segment, the participants from USEUCOM and its Service Components practiced completing their assigned events from the MESL. System operators from USEUCOM and its Service Components ensured that systems were functioning properly and practiced changing dates on the systems. Data collectors from the Directorate of Operational Test and Evaluation, Office of the Secretary of Defense, and the U.S. Air Force Operational Test and Evaluation Center practiced the data collection plan. Technicians from the Defense Information Systems Agency ensured that communications paths were working properly and worked to restore communications when failures occurred. None of the communications failures experienced during Part I were Y2K related; rather, they were the result of assembling a communications path where none previously existed and of weather.

Part I Baseline Segment. During the baseline segment, the systems were set to August 1, 1999. The participants completed the MESL events to have a baseline for determining whether Y2K failures occurred during the Y2K operations phase. USEUCOM had to run the baseline twice because of communications failures that were not Y2K related.

Part I Y2K Operations Segment. During each day of the Y2K operations segment, the technicians changed the dates on the systems clocks for the three critical date crossings and the participants completed the MESL events each day. The data collectors gathered and analyzed the data to determine whether any Y2K-related failures occurred. USEUCOM experienced a Y2K hard failure with the Windows End-to-End Force Tracking application of the Global Command and Control System-Army. USEUCOM used the operational contingency plan for the Global Command and Control System-Army and accomplished the task with no significant operational or time impact.

Part I Recovery Segment. During the recovery segment, the data collectors ensured that they had collected all data needed to assess Y2K operational readiness. The other participants reset systems to current-day operations to ensure that Y2K test data would not contaminate real-world data and certified that the systems contained no Y2K test data.

Air Operations-Part II. USEUCOM successfully completed the air operations part of its operational evaluation in June 1999 at Hurlburt Field, Florida. Part II was conducted jointly with the operational assessment by the Air Combat Command of the Air Operations Center. USEUCOM conducted Part II using seven response cells replicating an air operations center, a battlefield coordination element, a deep operations coordination cell, and a wing operations center at three locations in Europe and the United States. During the rehearsal, baseline operations, and Y2K operations segments, participants

completed 65 scripted events from the MESL using 10 thin-lines of systems to assess the ability of USEUCOM to complete the strategic and operational tasks related to air operations for NEO and peacekeeping operations (see Appendix C). Because of the criticality of the Contingency Theater Automated Planning System (CTAPS) to air operations, USEUCOM decided to include CTAPS version 5.2.3 in its operational evaluation even though that version had just gone through joint acceptance testing the week before and had not yet been fielded in the European theater.[5]

Part II Rehearsal Segment. During the rehearsal segment, the participants from Air Combat Command, USEUCOM, and its Service Components practiced completing their assigned events from the MESL. System operators ensured that systems were functioning properly and practiced changing dates on the systems. Data collectors from the Directorate of Operational Test and Evaluation, Office of the Secretary of Defense, and the U.S. Air Force Operational Test and Evaluation Center practiced the data collection plan. Technicians from the Air Combat Command ensured that communications paths were working properly and worked to restore communications when failures occurred. None of the communications failures experienced during Part II were Y2K related; rather, they were the result of an extremely short time frame available to set up the communications paths because of the limited availability of the test facility.

Part II Baseline Segment. During the baseline segment, the systems were set to December 31, 1999. The participants completed the MESL events to have a baseline for determining whether Y2K failures occurred during the Y2K operations phase. USEUCOM had to perform some of the MESL events after the initial baseline was completed because of communications and interface problems that were not Y2K related.

Part II Y2K Operations Segment. During each day of the Y2K operations segment, the technicians changed the dates on the systems clocks for the three critical date crossings and the participants completed the MESL events each day. The data collectors gathered and analyzed the data during the operational evaluation to determine whether any Y2K-related failures occurred. USEUCOM continued to experience communications and interface problems during this segment; however, USEUCOM was able to complete its MESL events each day. USEUCOM did not experience any Y2K-related failures; however, USEUCOM encountered three anomalies with CTAPS, one related to airlift data and two related to processing e-mail. However, by using its operational contingency plan, USEUCOM accomplished the airlift data task with no significant operational or time impact. Although the operational contingency plan was effective, USEUCOM planned to further review the contingency plan to refine procedures for intelligence functions of the Air Operations Center and to incorporate instructions into the contingency plan for the anomalies related to processing e-mail.

[5]The Joint Standard Air Operations Software Configuration Control Board unanimously voted to make CTAPS 5.2.3 the system of record for joint air operations at its July 15, 1999, meeting.

Part II Recovery Segment. During the recovery segment, the data collectors ensured that they had collected all data needed to assess Y2K operational readiness. The other participants reset systems to current-day operations to ensure that Y2K test data would not contaminate real-world data and certified that the systems contained no Y2K test data.

Intelligence Operations-Part III. USEUCOM successfully completed the intelligence part of its operational evaluation in August 1999 at the Joint Analysis Center[6] in the United Kingdom. Although the 66th Military Intelligence Group[7] was able to participate in Part I, the Joint Analysis Center was unable to participate in Parts I and II because it was involved in real-world operations and because it was in the process of fielding Y2K compliant systems. Therefore, USEUCOM was unable to fully evaluate the production and dissemination of order of battle and intelligence assessments until it completed Part III. USEUCOM conducted Part III using two response cells, one at the Joint Analysis Center and the other at USEUCOM headquarters. During the rehearsal, baseline, and Y2K operations segments, participants completed 14 scripted events from the MESL using 5 thin-lines of systems to assess the ability of USEUCOM to complete the strategic and operational tasks related to intelligence production and dissemination for NEO and peacekeeping operations (see Appendix C). USEUCOM and the Joint Analysis Center conducted Part III using five mission-critical systems: the Automated Message Handling System, the Intelink, the Joint Deployable Intelligence Support System-Client Server Environment, the Modernized Integrated Database System, and Windows NT. USEUCOM did not include the Linked Operations-Intelligence Centers Europe System[8] in Part III, even though it is the key NATO intelligence system in Europe and is the primary allied intelligence system in Bosnia. To complete its assessment of the Y2K readiness of intelligence operations, USEUCOM relied on the Defense Intelligence Agency tests of the Joint Worldwide Intelligence Communications System and the National Imagery and Mapping Agency tests of DoD standard intelligence systems, which were successfully completed during the summer of 1999.

Part III Rehearsal Segment. During the rehearsal segment, the participants from USEUCOM and the Joint Analysis Center practiced completing their assigned events from the MESL. System operators from USEUCOM and the Joint Analysis Center ensured that systems were functioning properly and practiced changing dates on the systems. Data collectors from the Directorate of Operational Test and Evaluation, Office of the

[6]The Joint Analysis Center provides intelligence information to coalition, NATO, and U.S. forces during peace, crises, and war.

[7]The 66th Military Intelligence Group provides intelligence information to USEUCOM. It is a USAREUR subordinate command, but also reports to the U.S. Army Intelligence and Security Command.

[8]The Linked Operations-Intelligence Centers Europe System provides NATO forces with the ability to electronically access, publish, and share NATO-releasable intelligence information. The USEUCOM Y2K Task Force certified the Linked Operations-Intelligence Centers Europe System as Y2K compliant on March 15, 1999.

Secretary of Defense, practiced the data collection plan. Technicians from USEUCOM and the Joint Analysis Center ensured that communications paths were working properly.

Part III Baseline Segment. During the baseline segment, the systems were set to December 31, 1999. The participants completed the MESL events to have a baseline for determining whether Y2K failures occurred during the Y2K operations phase.

Part III Y2K Operations Segment. During each day of the Y2K operations segment, the technicians changed the dates on the systems clocks for the three critical date crossings and the participants completed the MESL events each day. The data collectors gathered and analyzed the data to determine whether any Y2K-related failures occurred. USEUCOM did not experience any Y2K-related failures during the operations segment. However, USEUCOM encountered a problem with an expired password, which was not Y2K related.

Part III Recovery Segment. During the recovery segment, the data collectors ensured that they had collected all data needed to assess Y2K operational readiness. The other participants reset systems to current-day operations to ensure that Y2K test data would not contaminate real-world data and certified that the systems contained no Y2K test data.

NATO and Coalition Forces. USEUCOM was not tasked by the Joint Staff to include NATO or coalition forces in its operational evaluation; therefore, the operational evaluation did not assess the Y2K operational readiness of NATO or coalition forces' mission-critical systems supporting peacekeeping operations in the European theater. The USEUCOM operational evaluation plan states that NATO and coalition forces are not participating in the operational evaluation because it could not be arranged within the planning cycle. However, USEUCOM believed that the limitation was mitigated by Combined Endeavor 99, which took place in May 1999. Combined Endeavor 99 was a USEUCOM-sponsored exercise that tested the ability of NATO and Partnership for Peace[9] military staffs to communicate in a multi-Service, multi-national environment. Specifically, it tested the interoperability of switches, multi-channel radios, high frequency radios, and data networking equipment. However, Combined Endeavor 99 did not include any Y2K testing. The test results of Combined Endeavor 99 provided USEUCOM with sufficient information to assess its ability to interoperate, specifically to communicate, with NATO and coalition forces. However, because it did not address potential Y2K interoperability issues, Combined Endeavor 99 is of limited value to USEUCOM for assessing Y2K operational readiness. USEUCOM personnel stated that the USEUCOM Y2K Task Force and Supreme Headquarters Allied Powers Europe Y2K Programme

[9]Partnership for Peace is a NATO initiative to develop cooperative military relations for the purposes of joint planning, training, and exercises to strengthen the ability of member nations to undertake missions in peacekeeping, search and rescue, and humanitarian aid. The Partnership for Peace alliance has 27 member nations, including the states of the former Soviet Union.

Management Office are exchanging information on the status of systems as data become available. USEUCOM is working with NATO to resolve potential Y2K interoperability issues and needs to continue to take action through its risk mitigation efforts to reduce any potential impact on its ability to conduct peacekeeping operations caused by Y2K interoperability problems with NATO during the year 2000.

Analyzing the Operational Evaluation. USEUCOM conducted data analysis during and after the execution phase of each part of the operational evaluation to determine whether failures were Y2K related, to categorize failures as either hard or soft failures, and to determine the impact of failures on the mission. Based on the data analyses, the USEUCOM operational evaluation verified that mission-critical systems that had been certified as Y2K compliant functioned as expected in a Y2K environment. However, USEUCOM data analyses identified one Y2K-related failure in Part I and three non-Y2K-related system anomalies in Part II. USEUCOM data analysis did not identify any Y2K-related failures or anomalies during Part III.

Analysis of Part I. During Part I-land and sea operations, USEUCOM identified one Y2K hard failure in the Windows End-to-End Force Tracking application of the Global Command and Control System-Army. That application interfaces the Global Command and Control System-Army with the Joint Operational Planning and Execution System. A program management office representative was on site during the operational evaluation. After analyzing the failure, the program management office and the contractor developed a software patch for the failure and distributed the revised programming to USAREUR for further testing before the end of the operational evaluation. The program management office and USAREUR successfully tested the revised program and the program management office completed fielding the software patch in July 1999.

Analysis of Part II. During Part II-air operations, USEUCOM did not identify any Y2K failures; however, USEUCOM identified three anomalies that were not considered to be Y2K-related failures. One anomaly occurred when airlift data was imported from the Command and Control Information Processing System to the current operations module of CTAPS. When the airlift data was imported, it showed the year from the system date on the sending system rather than the year from the system date on the receiving system. The anomaly occurred when dates crossed from December 31 to January 1. Because the anomaly occurred during several different year crossings, USEUCOM determined that it was not Y2K related. USEUCOM also identified two other anomalies affecting the processing of e-mail in CTAPS that were not related to Y2K. Specifically, CTAPS was not sorting e-mails correctly and was not consistently transmitting e-mails. USEUCOM and Air Combat Command were working with the program manager to correct the three anomalies.

Analysis of Part III. During Part III-intelligence operations, USEUCOM did not identify any Y2K-related failures or anomalies. However, USEUCOM encountered a non-Y2K-related issue with an expired password because one of the participants did not extend the expiration date on his

password. When the Y2K rollover occurred, the computer system would not recognize his password; therefore, he could not gain access to the system and it appeared that he had lost data. During the execution of the operational evaluation, USEUCOM believed it to be a Y2K failure; however, analysis of the data after the operational evaluation determined that it was only an expired password, not a Y2K failure.

Reporting on the Operational Evaluation. After USEUCOM completed each part of the operational evaluation, it prepared reports and forwarded them to the Joint Staff in accordance with the Joint Staff Guide. USEUCOM prepared a preliminary report, dated May 25, 1999, for Part I; a final report, dated July 22, 1999, consolidating the results of Parts I and II; and an updated final report, dated September 21, 1999, summarizing the results of all three parts of the operational evaluation. The final report summarized the results of the execution and analysis phases of the operational evaluation, provided suggested courses of action, and described lessons learned. In the final report, USEUCOM recommended that the program manager ensure that the software patch for the Global Command and Control System-Army is installed on all servers. In addition, USEUCOM suggested that fielding plans for the Y2K compliant version of CTAPS should schedule fielding dates no later than November 15, 1999, and that U.S. Central Command and U.S. Pacific Command should include the Y2K compliant version of CTAPS in their operational evaluations.[10] USEUCOM lessons learned included using qualified system operators, having redundant communications paths, providing good power distribution and adequate power protection of critical equipment, and including program management offices in the planning and execution of the operational evaluation.

Success of the Operational Evaluation. The USEUCOM operational evaluation was successful in verifying that systems that were certified as Y2K compliant functioned as expected in a Y2K environment. The operational evaluation demonstrated that USEUCOM should be operationally ready to perform land, sea, air, and intelligence operations in support of NEO and peacekeeping operations in the year 2000 and beyond. However, the operational evaluation did not assess the full operational capabilities of USEUCOM. Specifically, USEUCOM only assessed the thin-lines of systems from USEUCOM headquarters (the sensor) to the Service Component level of a joint task force, not to all "shooters" as required by the Joint Staff Guide. USEUCOM relied on Service-sponsored systems integration tests and functional area end-to-end tests to provide Y2K operational readiness data for those systems that it did not test during its operational evaluation. In addition, USEUCOM did not include systems in the operational evaluation if Y2K compliant versions of those systems had not been fielded in the European theater at the time of the operational evaluation, with the exception of CTAPS. Again, USEUCOM relied on Service-sponsored systems integration tests and functional area end-to-end tests to provide Y2K operational readiness data for the systems that USEUCOM did not test during its operational evaluation.

[10]The U.S. Central Command included CTAPS in its operational evaluations; the U.S. Pacific Command did not.

Service-Sponsored Systems Integration Tests

USEUCOM, in coordination with the Joint Staff and the Services, reviewed the test results from Service-sponsored systems integration tests that took place in the summer of 1999 and assessed its Y2K operational readiness. The USEUCOM operational evaluation focused on actions and systems that crossed Service Component lines or interacted with joint systems. In a message March 15, 1999, USEUCOM stated that intra-Service tasks from the Service Component joint task force to subordinate forces and below were to be evaluated by the owning Services and that USEUCOM would review Service compliance efforts to ensure that the end-to-end operational capability is validated as required by the Joint Staff Guide.

Army Systems Integration Tests. USEUCOM and USAREUR identified 31 Army standard systems that were mission-critical to NEO and peacekeeping operations. As of September 30, 1999, the Army Y2K Web Database indicated that the Army had conducted tests on 30 of those systems and had determined that they were Y2K compliant. The Army was replacing one system, which was planned to be fielded by September 30, 1999. The replacement system had been certified as Y2K compliant.

Navy Systems Integration Tests. USEUCOM and U.S. Naval Forces Europe identified 12 Navy standard systems[11] that were mission-critical to NEO and peacekeeping operations. As of September 28, 1999, the DoD Y2K Database indicated that the Navy had conducted tests on eight of those systems and had determined that they were Y2K compliant. The other four systems were not in the DoD Y2K Database.

Air Force Systems Integration Tests. USEUCOM and U.S. Air Forces in Europe identified 30 Air Force standard systems[12] that were mission-critical to NEO and peacekeeping operations. As of July 19, 1999, the U.S. Air Force Evaluation Database indicated that the Air Force had conducted tests on all 30 of those systems and had determined that they were Y2K compliant.

USEUCOM analyzed the results of the Service-sponsored systems integration tests to determine that it would be operationally ready to perform NEO and peacekeeping operations in the year 2000. In addition, USEUCOM analyzed those test results and the test results from the functional area end-to-end tests to further determine the status of its Y2K operational readiness.

---

[11]The number of Navy standard systems does not include ships.

[12]The Combat Intelligence System was not included in the 30 Air Force systems because it was not Y2K compliant and was to be replaced by the Theater Battle Management Core System. USEUCOM tested the Target Weaponeering Module, the equivalent software module from the Theater Battle Management Core System, during Part II of its operational evaluation. The Target Weaponeering Module functioned properly in a Y2K environment. However, the Target Weaponeering Module had not been approved for fielding.

Functional Area End-to-End Tests

USEUCOM, in coordination with the Joint Staff and Principal Staff Assistants, reviewed test results of functional area end-to-end tests that took place in the summer of 1999 and assessed its Y2K operational readiness. According to the DoD Management Plan, the Principal Staff Assistants are responsible for conducting functional area end-to-end tests and verifying that all functions under their purview will continue unaffected by Y2K issues. During its operational evaluation, USEUCOM did not assess mission-critical systems for communications or logistics because it was relying on the functional area end-to-end tests to provide the data needed to adequately assess its operational readiness.

Communications. USEUCOM did not assess the Y2K operational readiness of communications[13] during its operational evaluation. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) memorandum, "Year 2000 Computer Problem Testing," April 5, 1999, prohibits DoD Components from live testing the Defense Information Infrastructure telecommunications networks. Because of that prohibition, USEUCOM was relying on the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) to assess the communications systems. That assessment was completed in June 1999. The final report, "Joint User Switch Exercise Year 2000 Assessment (JUSE 99-Y2K)," September 20, 1999, stated that no Y2K-related failures occurred during the assessment.

Logistics. During the operational evaluation, USEUCOM did not test the thin-lines of systems that supported the operational task of sustaining theater logistics because the Army had not fielded Y2K compliant versions of those systems in the European theater at the time of the operational evaluation. Logistical support in the European theater is predominantly a USAREUR function performed by the 21st Theater Support Command. The 21st Theater Support Command thin-lines of mission-critical logistics systems consisted of standard DoD and Army systems used to perform maintenance, supply, training, and transportation functions. As a result, USEUCOM and USAREUR decided to rely on DoD and Army testing to verify the operational capability of the thin-lines of systems for sustaining logistics in the European theater. For the two DoD systems,[14] both were tested as part of the logistics functional area end-to-end test in July 1999 and performed properly in a Y2K environment. All

[13]Those communications systems included Defense Switched Network, Unclassified but Sensitive Internet Protocol Router Network, Secret Internet Protocol Router Network, and satellites.

[14]The Global Command and Control System and Defense Automatic Addressing System.

nine Army systems[15] were tested as part of the Army Service-sponsored systems integration tests. The test results for those nine systems are documented in the following reports.

- The Project Manager for the Global Combat Support System-Army issued a final report, "PM GCSS-Army Year 2000 (Y2K) Level I End-to-End System Test Report for Mission-Critical Systems: ULLS-A, ULLS-G, SAMS-Rehost, SARSS-O, SAAS-Mod," July 1, 1999.[16] The report concluded that the test was satisfactory and that the systems performed as designed.

- The Army Materiel Command issued a final report, "U.S. Army Materiel Command Year 2000 End-to-End Test Level I and II Test Report," August 31, 1999. That report concluded that the systems tested were Y2K end-to-end test compliant.

- As of September 21, 1999, the Joint Interoperability Test Command had prepared a working draft report, "Logistics Year 2000 End-to-End Level II Exercise Evaluation Report," September 1999, which concluded that mission-critical logistics processes will continue unaffected by Y2K issues. However, a Y2K anomaly was identified for the Standard Army Ammunition System-Modernization; but, the operational impact of that anomaly was assessed as minimal and system representatives had a plan to correct the code and deliver a patch to the field by October 31, 1999.

In addition to communications and logistics, USEUCOM, in coordination with the Joint Staff and the Principal Staff Assistants, reviewed the functional area end-end test results on the Y2K status of health care, personnel, and intelligence and determined that there would be no impact on USEUCOM Y2K operational readiness. Although USEUCOM did not include health care and personnel in its thin-lines of mission-critical systems needed for completing NEO and peacekeeping operations, those functional areas are essential to maintaining the overall readiness of the Armed Forces in the European theater.

USEUCOM completed its assessment of Y2K operational readiness in the European theater and determined that it is operationally ready to perform NEO and peacekeeping operations in the Y2K environment. However, USEUCOM was still in the process of identifying factors external to DoD that could affect its operational readiness, such as Y2K compliance issues of NATO and coalition forces. Once those factors are identified, USEUCOM plans to take action to reduce any potential impact of those external factors through risk mitigation efforts.

[15]Those systems are four subsystems of the Standard Army Ammunition System (SAAS) (Ammunition Supply Point, Ammunition Transfer Point, Division Ammunition Office, and Modernization), two subsystems of the Unit Level Logistics System (ULLS) (Air and Ground), and three subsystems of the Standard Army Retail Supply System (SARSS) (1, 2A, and 2C).

[16]Acronyms in the title of the report not defined in footnote 15 are Project Manager (PM), Global Combat Support System (GCSS), and Standard Army Maintenance System (SAMS).

USEUCOM Risk Mitigation Efforts

In addition to the operational evaluation, USEUCOM planned to conduct risk mitigation efforts. Specifically, USEUCOM planned to conduct a tabletop exercise in October 1999 to assess Y2K risk to mission-essential and non-mission-essential operations and to coordinate and deconflict contingency plans across the European theater to ensure continuity of operations and life support (such as communications and utilities) should disruptions in host nation support occur. In addition, the tabletop exercise should ensure that the Service Components review their contingency plans. USEUCOM planned to cover the following areas:

- communications (internal and external) systems;
- computer systems (software);
- mission-essential and non-mission-essential operations; and
- utilities (electrical power, water, waste water, and heat) and lines of communication (airports, sea ports, rail systems, and road/truck systems).

The tabletop exercise will consist of three phases: risk assessment, contingency plan review, and risk assessment considering mitigation. During the risk assessment phase, participants will develop an overall European theater risk assessment. During the contingency plan review phase, the participants will review specific areas of contingency plans covering the two highest operational risk areas across Service Components for risk mitigation and deconfliction of resources. During the risk assessment considering mitigation phase, participants will assess residual risk based on identified risks and risks that have been mitigated through contingency planning. USEUCOM planned to use requests for information, commercial studies, local information from utility providers, and the DoD Y2K Database to assist in identifying risks. However, USEUCOM did not plan to include Y2K compliance data on NATO or coalition forces' mission-critical systems supporting peacekeeping operations. USEUCOM expects to brief the results of the tabletop exercise at the Component Commanders Conference in October 1999. As part of the risk mitigation process, USEUCOM planned to factor in the results from its operational evaluation, the Service-sponsored systems integration tests, and the functional area end-to-end tests to ensure that all elements are covered and that potential Y2K failures will result in as little disruption as possible. However, to complete its risk mitigation efforts, USEUCOM needs to take action to reduce any potential impact on its ability to conduct peacekeeping operations caused by disruptions in host nation support or Y2K interoperability problems with NATO or coalition forces during the year 2000.

Conclusion

The combination of the USEUCOM operational evaluation, Service-sponsored systems integration testing, and functional area end-to-end testing provided high assurance that USEUCOM will be operationally ready to perform NEO and peacekeeping operations in the year 2000. However, USEUCOM needs to continue to focus on potential Y2K interoperability problems with NATO and coalition forces that could adversely affect its operational readiness. USEUCOM must be operationally ready to support efforts to sustain peaceful settlements among belligerent parties as well as effectively remove civilian non-combatants quickly and safely from threatened areas.

Recommendation and Management Comments

We recommend that the Commander in Chief, U.S. European Command, through the Year 2000 Task Force include, in risk mitigation efforts, a focus on year 2000 compliance of North Atlantic Treaty Organization and coalition forces' mission-critical systems supporting peacekeeping operations in the European theater.

USEUCOM Comments. USEUCOM generally agreed with the report and stated that its risk mitigation efforts encompass contingency planning for infrastructure and host nation support risks to operations and to life support of military communities, ensurance of continuity of operations of ongoing operations, and engagement with NATO and coalition forces' risk mitigation activities. USEUCOM stated that a number of information sources were being tapped, including U.S. intelligence sources, to assess the risks. However, in recognition of the limited information available on the actual status of other nations' command and control systems, planning by USEUCOM and its Service Components will continue to include the risk that all or parts of those systems may not be available. In its determination of the risks to be mitigated, USEUCOM will include all available data on the compliance of NATO and coalition forces' mission-critical systems with which USEUCOM must interoperate. The USEUCOM Y2K Task Force and Supreme Headquarters Allied Powers Europe Y2K Programme Management Office are exchanging information on the status of systems as data become available.

Appendix A. Audit Process

This report is one in a series being issued by the Inspector General, DoD, in accordance with an informal partnership with the Chief Information Officer, DoD, to monitor DoD efforts to address the Y2K computing challenge. For a listing of audit projects addressing this issue, see the Y2K web pages on IGnet at http://www.ignet.gov/.

Scope

We reviewed DoD and Joint Staff guidance on planning and executing operational evaluations and the planning documents that USEUCOM prepared for its operational evaluation and for its risk mitigation efforts dated from December 1998 through September 1999. In addition, we reviewed DoD guidance on conducting Service-sponsored systems integration tests and functional area end-to-end tests dated from December 1998 through June 1999. We also observed Parts I and II of the USEUCOM operational evaluation. We reviewed material related to planning for and reporting on Part III of the operational evaluation and subsequent risk mitigation data collection and analysis.

Part I. The following organizations took part in Part I of the operational evaluation. Participating at the Warrior Preparation Center in Einsiedlerhof Air Station, Germany, were USAREUR; Southern European Task Force; and the Global Command and Control System-Army Program Management Office. The Southern European Task Force also participated with the 66th Military Intelligence Group in Darmstadt, Germany. U.S. Naval Forces Europe participated at the Warrior Preparation Center and from its headquarters in London, England. In addition, the USS *Inchon* (MCS 12) participated while underway. The U.S. Marine Forces Europe participated at the Warrior Preparation Center and the 22nd Marine Expeditionary Unit participated from Camp Lejuene, North Carolina. The Special Operations Command Europe participated at the Warrior Preparation Center.

Part II. The following organizations took part in Part II of the operational evaluation. The Air Combat Command; Electronic Systems Center; Pacific Air Forces; U.S. Air Forces Central Command; U.S. Air Forces in Europe; USAREUR; and USEUCOM participated at Hurlburt Field, Florida. The U.S. Naval Forces Europe participated from its headquarters in London. The Air Combat Command and U.S. Air Forces in Europe participated at Eglin Air Force Base, Florida.

Part III. USEUCOM and the Joint Analysis Center were the only organizations that took part in Part III.

The Directorate of Operational Test and Evaluation, Office of the Secretary of Defense, and the Warrior Preparation Center provided personnel to perform data collection during all parts of the operational evaluation. The Defense Information Systems Agency provided technical personnel during Part I; the U.S. Air Force Operational Test and Evaluation Center provided personnel to perform data collection during Parts I and II; and the Air Combat Command provided technical personnel during Part II.

Limitations to Audit Scope. During the audit, we did not validate the Y2K compliance data that we obtained from the DoD and Service databases; rather, we relied on the Services to enter accurate data into the databases. In addition, we did not validate the results of functional area end-to-end tests because we relied on the organizations conducting the tests to provide accurate test results.

DoD-Wide Corporate-Level Goals. In response to the Government Performance and Results Act, DoD has established 6 DoD-wide corporate-level performance objectives and 14 goals for meeting the objectives. This report pertains to achievement of the following objectives and goals.

- **Objective:** Prepare now for an uncertain future. **Goal:** Pursue a focused modernization effort that maintains qualitative superiority of the United States in key war fighting capabilities. **(DoD-3)**

- **Objective:** Maintain highly ready joint forces to perform the full spectrum of military activities. **Goal:** Maintain high military personnel and unit readiness. **(DoD-5.1)**

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to achievement of the following objectives and goals in the Information Management Functional Area.

- **Objective:** Become a mission partner. **Goal:** Serve mission information users as customers. **(ITM-1.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Modernize and integrate Defense information infrastructure. **(ITM-2.2)**

- **Objective:** Provide services that satisfy customer information needs. **Goal:** Upgrade technology base. **(ITM-2.3)**

High-Risk Area. In its identification of risk areas, the General Accounting Office has specifically designated risks in resolution of the Y2K problems as high. This report provides coverage of that problem and of the overall Information Management and Technology high-risk area.

Methodology

During the audit, we evaluated the progress that USEUCOM had made in evaluating its ability to perform NEO and peacekeeping operations in the year 2000. We focused our review of the USEUCOM operational evaluation on USEUCOM planning and execution efforts. We reviewed USEUCOM preparations for its operational evaluation, which took place from December 1998 through April 1999, to determine whether USEUCOM planned and executed its operational evaluation in accordance with the DoD Management Plan and the Joint Staff Guide. We interviewed personnel from the Directorate of Operational Test and Evaluation, Office of the Secretary of Defense; the Joint Staff; USEUCOM and its Service Components; and the Defense Information Systems Agency to determine their level of involvement in planning and executing the operational evaluation. In addition, we reviewed the USEUCOM preliminary after-action report for Part I, May 25, 1999; the final after-action report for Parts I and II, June 22, 1999; the consolidated final after-action report for all parts of the operational evaluation, September 21, 1999; and the draft after-action report for Combined Endeavor 99, issued August 1, 1999.

Use of Computer-Processed Data. We obtained test results from the DoD Y2K Database, the Army Y2K Web Database, and the Air Force Evaluation Database to determine whether systems not included in the USEUCOM operational evaluation had been included in either Service-sponsored systems integration tests or functional area end-to-end tests. We also used data from those databases to determine Y2K compliance status of the systems. We did not establish the reliability of the data because it was beyond the scope of our audit; rather, we relied on the Services to enter accurate data into the databases. However, not establishing the reliability of the databases will not affect the conclusions we reached on the results of the USEUCOM operational evaluation.

Audit Type, Dates, and Standards. We performed this program audit from April through September 1999 in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program. We did not review the management control program related to the overall audit objective because DoD recognized the Y2K issue as a material management control weakness area in the FY 1998 Annual Statement of Assurance.

Appendix B. Summary of Prior Coverage

The General Accounting Office and the Inspector General, DoD, have conducted multiple reviews related to Y2K issues. General Accounting Office reports can be accessed over the Internet at http://www.gao.gov. Inspector General, DoD, reports can be accessed over the Internet at http://www.dodig.osd.mil. The following previous reports are of particular relevance to the subject matter in this report.

Inspector General, DoD

Report No. 99-254, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility: Operational Evaluation Planning by U.S. Forces Korea," September 16, 1999.

Report No. 99-245, "Year 2000 Issues Within the U.S. Pacific Command's Area of Responsibility: Operational Evaluation Planning at U.S. Pacific Command Headquarters," September 2, 1999.

Report No. 99-145, "Year 2000 Issues Within U.S. European Command and Its Service Components," April 30, 1999.

Report No. 99-141, "Year 2000 Issues Within U.S. Central Command and the Service Components," April 22, 1999.

Report No. 99-059, "Summary of DoD Year 2000 Conversion - Audit and Inspection Results," December 24, 1998.

Army Audit Agency

Memorandum Report No. AA 98-292, "U.S. European Command's Management of the Year 2000," July 30, 1998.

Appendix C. Strategic and Operational Tasks Assessed in Operational Evaluation

During the operational evaluation, USEUCOM assessed its thin-lines of mission-critical systems that supported its ability to accomplish the following strategic tasks (ST) and operational tasks (OP) associated with its critical missions of NEO and peacekeeping operations.

ST 1.1 Conduct Strategic Deployment. To move (shift, deploy) joint or multinational forces to more advantageous positions relative to the enemy.

OP 1.1 Conduct Operational Movement. To deploy, shift, regroup, or move joint or multinational operational formations within a theater of operations or a joint operations area from less promising to more promising locations relative to enemy locations.

ST 1.1.1 Process Requests for Forces to be Deployed. To review and approve a request from a subordinate commander for forces from outside the subordinate commander's theater of operations into the subordinate commander's area.

OP 1.1.1 Formulate Request for Strategic Deployment to Theater of Operations or Joint Operations Area. To prepare a request to the theater combatant commander for the strategic movement of joint/multinational operational forces from outside the theater of operations or joint operations area (JOA).

ST 1.1.2 Provide Theater Strategic Reception, Staging, Onward Movement, and Integration. To receive units, personnel, equipment, and material in theater and to process and move them to a transferable point to the responsible operational commander, available for battle.

OP 1.1.2 Conduct Intratheater Deployment and Redeployment of Forces Within Theater of Operations or JOA. To relocate or move operational forces by any means or mode of transportation within a theater of operations or JOA preparatory to deploying the force into combat formation in support of the joint force commander's plan.

ST 1.1.3 Conduct Intratheater Deployment of Forces. To deploy or move a joint or multinational force by any means of transportation from its position within the theater to another position within the theater or to another theater of war in support of the theater combatant commander's strategic plan.

ST 1.3.3 Synchronize Forcible Entry in Theater of War. To synchronize the seizure and holding of a military lodgment. This is often the only method of gaining access into the operational area or for introducing forces into the region. It requires adapting forces to fit the purpose of synchronizing forcible entry. The forces are scheduled for simultaneous deployment and employment in the theater of war.

OP 1.2.4.3 Conduct Forcible Entry: Airborne, Amphibious, and Air Assault. To conduct operations to seize and hold a military lodgment in the face of armed opposition, to strike directly at enemy operational or strategic centers of gravity, or to gain access into a theater of operations or JOA or for introducing decisive forces into the region.

ST 1.6 Control or Dominate Strategically Significant Areas. To dominate or control the physical environment (air, land, sea, and space). The possession of the physical environment gives the holder a strategic advantage.

OP 1.5.3 Gain and Maintain Air Superiority in Theater of Operations or JOA. To gain control of the air to the degree which permits the conduct of operations by air, land, and sea forces at a given time and place without prohibitive interference by the opposing force in the theater of operations or JOA.

ST 3.1.1 Select Strategic Targets in the Theater for Attack. To analyze each strategic target to determine if and when it should be attacked for maximum effect on enemy center of gravity, strategic decisive point, and in conformance with the combatant commander's strategic concept and intent. The destruction and degradation of enemy information warfare and weapons of mass destruction production, infrastructure, and delivery systems are included in this strategic task.

OP 3.1 Conduct Joint Force Targeting. To positively identify and select air, land, and sea targets that decisively impact campaigns and major operations and match the targets to appropriate joint or multinational operational firepower.

OP 3.1.1 Establish Joint Force Targeting Guidance. To provide joint force commander's guidance and priorities for targeting and identification of requirements by Components; the prioritization of those requirements; the acquisition of targets or target sets; and the attack of targets by Components.

ST 3.1.3 Conduct Theater Combat Assessment. Includes all force employment for strategic objectives. This task also includes assessing theater battle damage, munitions effects, and reassessing mission requirements (for example, reattack the target).

OP 3.1.3 Develop Operational Targets. To evaluate and choose operational targets for attack to achieve optimum effect on enemy decisive points and centers of gravity consistent with the operational-level joint force commander's intent.

OP 3.1.4 Prioritize High-Payoff and High-Value Targets. To rank high-payoff targets and high-value targets in the order of their importance and select attack sequence for attacking decisive points and defeating enemy centers of gravity within the context of the commander's campaign plan.

OP 3.1.5 Publish Tasking Orders for Employment of Air Assets and Other Means. To assign missions and specific taskings to each joint force subordinate command employing air assets or other means in the airspace control area of the area of responsibility or JOA. Typically, this task pertains to the air tasking order.

ST 4.2 Coordinate Support for Forces in Area of Responsibility. To provide units and replacements that are both trained and organizationally sound. Also, provide personnel services and health services to support theater strategy, campaigns, and routine communications zone.

OP 4.5.1 Provide for Movement Services in Theater of Operations or JOA. To move personnel, equipment, and supplies to sustain campaigns and major operations and to provide transportation resources for moving the forces that execute those operations.

OP 4.6 Build and Maintain Sustainment Bases. To build and maintain principal and supplementary bases of support for theater of operations sustainment activities in conformance with theater combatant commander's guidance.

ST 5 Provide Theater Strategic Command and Control. Includes the development and revision of theater strategy based upon national security strategy and National Military Strategy. A theater strategy is designed to accomplish a desired strategic result by matching objectives, threats, and opportunities in light of resource limitations.

ST 5.1 Operate and Manage Theater Communications and Information Systems. To receive strategic direction or orders from national levels, obtain information for the combatant commander or staff, and communicate the information to those who need it to accomplish combatant commander objectives. This task includes interfacing with friendly and enemy civilian government authorities in the theater. It also includes the translation, retention, and dissemination of all types of information.

OP 5.1.1 Communicate Operational Information. To send and receive operationally significant data from one echelon of command to another by any means.

OP 5.2 Assess Operational Situation. To evaluate information received through reports or the personal observations of the commander on the general situation in the theater of operations and conduct of the campaign or major operation.

OP 5.3 Prepare Plans and Orders. To make detailed plans, staff estimates, and decisions for implementing the theater combatant commander's theater strategy, associated sequels, and anticipated campaigns or major operations.

ST 5.3.4 Prepare and Coordinate Theater Strategy, Campaign Plans or Operation Plans, and Orders. To develop a plan or order that proclaim the theater strategic concept and intent of the theater combatant commander and the National Command Authority's National Military Strategy (and multinational military strategy where appropriate) and plans. Plans and orders include rules of engagement and other restrictions and constraints. This task also includes host nation support.

ST 6.2 Provide Protection for Theater Strategic Forces and Means. To reduce or avoid the effects of enemy and unintentional friendly actions. In military actions other than war, this task includes protecting civil and government infrastructure. This task also includes the protection of non-combatant evacuees prior to departure from theater.

USEUCOM only partially assessed its thin-lines of mission-critical systems that supported its ability to accomplish the following strategic task because NATO and coalition forces did not participate in the operational evaluation.

ST 8.2.10 Establish/Participate in Joint, Combined, or Multinational Operations Within Area of Responsibility. To ensure mutual support and consistent effort in the area of responsibility by coordinating with allies and coalition partners and appropriate international organizations. Effective coordination is achieved when all parties understand and agree to the desired end state, concept of operations, intent, objectives, priorities, and support requirements.

ST 2 Develop Theater Strategic Intelligence, Surveillance, and Reconnaissance. To address the threat across the range of military operations including military operations other than war. Theater strategic intelligence includes determining when, where, and in what strength the enemy will set up to conduct theater-level campaigns and strategic unified operations. Also, this task provides surveillance and reconnaissance support to subordinate commanders and to designated national agencies.

OP 2.1 Plan and Direct Operational Intelligence Activities. To assist theater and joint task force commanders in determining their intelligence requirements, then planning the operational collection effort and issuing the necessary orders and requests to intelligence organizations.

OP 2.1.2 Determine and Prioritize Operational Information Requirements. To identify those items of information that must be collected and processed to develop the intelligence required by the commander's Priority Intelligence Requirements.

OP 2.1.3 Prepare Operational Collection Plan. To develop a collection plan that will satisfy the commander's intelligence requirements. Includes assigning the appropriate collection capabilities to fulfill specific intelligence requirements.

OP 2.1.4 Allocate Intelligence Resources in Theater of Operations or JOA. To assign adequate resources to theater and joint task force intelligence organization to permit the accomplishment of assigned intelligence tasks. Includes requesting support from national intelligence agencies and from allied countries.

OP 2.2.1 Collect Information on Operational Situation. To obtain operational information on enemy force strengths and vulnerabilities, threat operational doctrine, and forces. Includes collecting information to protect against assassinations, espionage, international terrorist activities, or sabotage.

OP 2.2.2 Directly Support Theater Strategic Surveillance and Reconnaissance Requirements. To provide, as directed, surveillance and reconnaissance support to combatant commanders and national-level agencies. This task includes providing the output of theater of operations or JOA assets or asset production to meet the needs of combatant commanders and designated national agencies.

OP 2.3 Process and Exploit Collected Operational Information. To convert collected operational information into forms that can be readily used by intelligence analysts during production.

OP 2.3.1 Conduct Technical Processing and Exploitation in Theater of Operations or JOA. To perform activities such as data conversion, decryption of encoded material, document translation, imagery development and interpretation, and technical analysis of captured enemy material.

OP 2.4.2 Prepare Intelligence for Theater of Operations or JOA. To prepare intelligence data and present them to the users, including other intelligence personnel, in a finished state.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition and Technology
  Director, Defense Logistics Studies Information Exchange
Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Policy
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense (Command, Control, Communications, and Intelligence, Surveillance, Reconnaissance, and Space)
  Deputy Chief Information Officer and Deputy Assistant Secretary of Defense (Chief Information Officer Policy and Implementation)
    Principal Director for Year 2000
Director, Operational Test and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Chief Information Officer, Army
Commanding General, U.S. Army, Europe, and Seventh Army
Inspector General, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Navy
Commander in Chief, U.S. Naval Forces Europe
Inspector General, Department of the Navy
Auditor General, Department of the Navy
Inspector General, Marine Corps

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Air Force
Commander, U.S. Air Forces in Europe
Inspector General, Department of Air Force
Auditor General, Department of the Air Force

Unified Commands

Commander in Chief, U.S. European Command
Commander in Chief, U.S. Pacific Command
Commander in Chief, U.S. Atlantic Command
Commander in Chief, U.S. Southern Command
Commander in Chief, U.S. Central Command
Commander in Chief, U.S. Space Command
Commander in Chief, U.S. Special Operations Command
Commander in Chief, U.S. Transportation Command
Commander in Chief, U.S. Strategic Command

Other Defense Organizations

Director, Defense Contract Audit Agency
Director, Defense Information Systems Agency
  Inspector General, Defense Information Systems Agency
  Chief Information Officer, Defense Information Systems Agency
  United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
  Inspector General, National Security Agency
Inspector General, Defense Intelligence Agency
Inspector General, National Imagery and Mapping Agency
Inspector General, National Reconnaissance Office

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs
General Accounting Office
  National Security and International Affairs Division
    Technical Information Center
  Accounting and Information Management Division
    Director, Defense Information and Financial Management Systems

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Special Committee on the Year 2000 Technology Problem
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Committee on Science

U.S. European Command Comments

Final Report Reference

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128

8 Sep 1999

MEMORANDUM FOR ECCM

FROM: ECJ3-Y2K

SUBJECT: Comments on draft DODIG Report on U S European Command Year 2000 Operational Readiness (TF Y2K), Project No 8LG-5093 02 dated, 11 Aug 99

1 The DoD IG Draft Audit Report is overall accurate and pertinent as of the cut-off date of 31 July 1999 HQ EUCOM J3-Y2K has a small number of editorial comments and offers an update of the operational evaluation progress since the cut-off date in response to the findings and recommendations in the report.

2 Editorial Comments:

a Page 2, footnote 2 – The definition of peacekeeping operations, as given, might easily be confused with peacemaking. For clarity, the definition from Joint Pub 3-07 might be better *"Military operations undertaken with the consent of all major parties to a dispute, designed to monitor and facilitate implementation of an agreement (cease fire, truce, or other such agreement) and support diplomatic efforts to reach a long-term political settlement."* — Revised

(For consistency, on the same page, footnote 1 – The definition for noncombatant evacuation operations in the footnote is essentially correct, however, the Joint Pub 3-07 definition might be used: *"Operations conducted to relocate threatened noncombatants from locations in a foreign country. These operations normally involve US citizens whose lives are in danger, and may also include selected foreign nationals."* — Revised

b Page 5, fourth paragraph – "Master Scenario Events List (MSEL)" The USEUCOM evaluation series used a Master Events Sequence List (MESL), the listing which sequenced the functional events of the evaluation Each functional event has an operator script, which was linked through a supporting database to the MESL — Revised

c Page 10, first paragraph and footnote 7 – "The Linked Operations Capability – Europe" should read "Linked Operations-Intelligence Centers Europe" — Revised

d Page 16, last paragraph – consistent with the definition of peacekeeping operations, the last line " to support efforts to achieve peaceful settlements " should read " to support efforts to sustain peaceful settlements " — Revised Page 18

e Page 25, fifth paragraph – "ST 8 2 10 Coordinate Multinational Operations Within Area of Responsibility" should read "ST 8 2 10 Establish/Participate in Joint, Combined, or Multinational Operations" Only joint operations were required in the USEUCOM evaluation — Revised Page 27

3 Update of status related to the findings and recommendations in the draft report:

a Findings

(1) " *the U.S. European Command needs to obtain the results of year 2000 tests* — Updated

occurring in the summer of 1999 to fully assess the year 2000 operational readiness Specifically, the U S. European Command needs to complete the operational evaluation of intelligence systems at the Joint Analysis Center and needs the test results from Service-sponsored systems integration tests and functional area end-to-end tests."

USEUCOM successfully conducted the operational evaluation of intelligence systems at the Joint Analysis Center from 13-16 August 1999. This evaluation completed the evaluation of the Command's thin-line of systems for the non-combatant operations and peacekeeping operations missions at and above joint task force level In coordination with the Joint Staff, the Command reviewed the evaluation status of each of the thin-line systems above joint task force level and confirmed that each of these systems had been evaluated at least twice The Command is currently working with the Components to validate the contents of the listing of thin-line systems below joint task force level and to confirm that each of these systems and other mission-critical systems have been evaluated at least once The Command target for completion of the review is 1 December 1999

(2) *"..the U.S. European Command needs to take action through its risk mitigation efforts to reduce any potential impact on its ability to conduct peacekeeping operations caused by year 2000 interoperability problems with the North Atlantic Treaty Organization and coalition forces"*

The Command's risk mitigation efforts encompass contingency planning for infrastructure and host nation support risks to operations and life support to military communities, assurance of continuity of operations of on-going operations and engagement with North Atlantic Treaty Organization and coalition forces risk mitigation activities A number of information sources are being tapped, including U S intelligence sources, to assess the risks In recognition, however, of the limited information that will be available on the actual status of other nations' command and control systems, Command and Component planning will continue to include the risk that all or parts of those systems are not available.

b Recommendations: (...that USCINCEUR, through the Year 2000 Task Force)

(1) *"Complete Part III of the operational evaluation of intelligence systems"*

USEUCOM successfully conducted the operational evaluation of intelligence systems at the Joint Analysis Center from 13-16 August 1999, as discussed above.

(2). *"Include in risk mitigation efforts year 2000 compliance data on North Atlantic Treaty Organization and coalition forces' mission-critical systems supporting peacekeeping operations in the European theater."*

The Command is including, in the determination of the risks to mitigate, that data which can be made available on the compliance of North Atlantic Treaty Organization and coalition forces' mission-critical systems with which the Command must operate The USEUCOM Y2K Task Force and SHAPE Y2K Programme Management Office are exchanging information on the status of these systems as it becomes available

4 Our POC for this report is Mr Emil Hunziker, DSN 430-6551

Bruce C Deary

BRUCE C. DEARY, Lt Col, USAF
Deputy Director Y2K Task Force

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report. Personnel of the Office of the Inspector General, DoD, who contributed to the report are listed below.

Shelton R. Young
Raymond D. Kidd
Evelyn R. Klemstine
Catherine M. Schneiter
Donney J. Bibb
Bryon J. Farber
Mary A. Hoover

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: U. S. European Command Year 2000 Operational Readiness

B. DATE Report Downloaded From the Internet: 02/10/99

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph #): **OAIG-AUD (ATTN: AFTS Audit Suggestions)**
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2884

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
DTIC-OCA, Initials: __VM__ **Preparation Date 02/10/99**

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.